REMARKS

Claims 1-22 and 25-44 are the pending in this application. In the Office Action, the Examiner rejected all of these claims under 35 U.S.C. 103 as being unpatentable over the prior art. Specifically, Claims 1-5, 7-23 and 26-42 were rejected as being unpatentable over U.S. Patent 6,453,296 (Iwamura) in view of a document "Introducing Trusted Third Parties to the Mobile Agent Paradigm" (Wilhelml, et al.). Claims 6 and 25 were rejected as being unpatentable over Iwamura in view of Wilhelml, et al. and further in view of U.S. Patent 6,714,982 (McDonough, et al.). Claims 43 and 44 were rejected as being unpatentable over Iwamura in view of Wilhelml and further in view of U.S. Patent 6,643,701 (Aziz). The Examiner also noted an informality in Claim 44 and required correction thereof.

Applicants are herein amending independent Claims 1, 31, 33, 34, 37 and 40 to better define the subject matters of these claims. Claim 43, which is dependent from Claim 1, is being amended to remove features being added to Claim 1 and to keep the language of Claim 43 consistent with the language of Claim 1, from which Claim 43 depends, and the informality that the Examiner noted in Claim 44 is being corrected.

In the Office Action, the Examiner also noted an informality in Claim 44, and this opportunity is being taken to correct that informality. In particular, the last line of the claim is being amended to correct the spelling of "the," so that this line now reads "...including that the client has properly authenticated." In view of this change, the Examiner is asked to reconsider and to withdraw the objection to Claim 44.

In addition, for the reasons discussed below, f Claims 1-22 and 25-44 patentably distinguish over the prior art and are allowable. The Examiner is thus also asked to reconsider and to withdraw the rejection of Claims 1-22 and 25-44 under 35 U.S.C. 103, and to allow these

claims. Generally, these claims patentably distinguish over the prior art because the prior art does not disclose or suggest the use of a double pair of private/public key pairs, in combination with a certificate authority, to authenticate communications to a user from a co-server, as described in independent Claims 1, 31, 33, 34, 37 and 40.

To elaborate, the present invention, generally, relates to procedures for improving the security of transactions using the world wide web. As explained in detail in the present application, this is done, in accordance with the instant invention, by enabling a server operator, operating within the existing SSL and Web infrastructure, to provide services with security properties that a remote user can verify. An important feature of the invention is that secure application software, loaded into a trusted co-server, can prove itself – that is, that this is the software running inside the trusted co-server – to arbitrary third parties.

To do this, the co-server is provided with a first, or device, private/public key pair. Then, after the application software is installed on the co-server, that software generates a second, or application, key pair including a public key and a private key. Next, the co-server application's ability to authenticate itself and the device key pair are used to prove to a certificate authority that the application key pair belongs to an installation of the co-server application.

The certificate authority then issues a certificate attesting to the public key of the application key pair and the entity to which that public key belongs. This certificate is stored on the co-server. Then, when a session is established between the client and the co-server application, the client is informed that this co-server application has knowledge of the private key of the application key pair to provide assurance of the authenticity of communications from the trusted co-server.

The prior art does not disclose or suggest the use of this double key pair, in combination with the certificate issued from a certificate authority to provide assurance to a user of the authenticity of communications from the trusted co-server.

For example, Iwamura describes a special purpose distributed system to support a particular agency's commerce application, and this system uses shared secrets and has the agency distribute secret keys, which make it impossible for the parties involved to prove non-repudiation. There is no disclosure, however, of the use of a first key pair to obtain a certificate attesting to a second key pair that is then used to authenticate communications from a trusted co-server.

Wilhelml discloses a trusted and tamper-resistant hardware device with a manufacture-certified key pair. However, Wilhelml uses this key pair to protect a remote shopping agent from malicious behavior.

Independent Claims 1, 31, 33, 34, 37 and 40 are being amended herein to describe the above-discussed feature of this invention. In particular, claims 1, 31, 33 and 40 describe the features that a device private/public key pair is installed on the co-server, and that the co-server application software generates an application key pair including a public key and a private key. These claims also describe the features that this device key pair, and the co-server application's ability to authenticate itself are used to prove to a certificate authority that the application key pair belongs to an installation of the co-server application, and that the co-server demonstrates to the client knowledge of the private key of the application key pair to provide assurance of the authenticity of communications from the trusted co-server.

Claims 34 and 37 describe similar features. In particular, these claims describe the features that a device private/public key and co-server application software is installed in the trusted co-server, and that this software generates an application key pair including a private key. These

claims describe the additional features that the co-server authenticates itself using the device key pair to prove to a certificate authority that the application key pair belongs to an installation of the co-server application, that the certificate authority issues a certificate attesting to the public key of the application key pair and the entity to which the public key belongs, and that the co-server application stores that certificate. As described in Claims 34 and 37, when a session is established between the client and the co-server application, the client is informed that the co-server application has knowledge of the private key of the application key pair to provide assurance of the authenticity of communications from the trusted co-server.

The above-discussed features of the present invention are of utility because they help to achieve a universal infrastructure that supports myriad applications from multiple server operators. The invention permits the additional flexibility of allowing the server operator, remote users, server application developers, hardware manufacturers, and SSL CAs all to be separate parties.

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also fail to disclose or teach the use of the double key pair, in combination with the authority certificate, to provide assurance of the authenticity of communications from the trusted co-server, in the manner described in Claims 1, 31, 33, 34, 37 and 40.

For instance, McDonough does not teach how the users can verify that the server operator is not lying or mistaken when the server operator claims the scanning has been performed.

Aziz discloses a procedure to provide secure communications over the Internet. This reference, though, does not suggest obtaining and using a certificate from a certificate authority as a certificate is obtained and used in the present invention, as explained above.

Because of the above-discussed differences between Claims 1, 31, 33, 34, 37 and 40 and the prior art, and because of the advantages associated with those differences, these claims patentably distinguish over the prior art and are allowable. Claims 2-22, 25-30, 43 and 44 are dependent from Claim 1 and are allowable therewith. Claim 32 is dependent from, and is allowable with, Claim 31; and Claims 35 and 36 are dependent from Claim 34 and are allowable therewith. Similarly, Claims 38 and 39 are dependent from Claim 37 and are allowable therewith; and Claims 41 and 42 are dependent from, and are allowable with, Claim 40.

In light of the above-discussion, the Examiner is asked to reconsider and to withdraw the objection to Claim 44 and the rejections of Claims 1-22 and 25-44 under 35 U.S.C. 103, and to allow these claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is requested to telephone the undersigned.

Respectfully submitted,

John S. Sensny

John S. Sensny
Registration No. 28,757
Attorney for Applicants

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy